在ASA或FTD升級到強化版本2026年9月後，排除VPN負載平衡集群形成故障

目錄

- 問題
- 環境
- 解析
  - 選項 1:完成升級（推薦）
  - 選項 2:無中斷升級方法（僅限ASA）
  - 驗證步驟
- 原因
- 相關內容

問題

將Cisco ASA或FTD裝置升級到Hardening Release 2026年9月發佈的一個版本後，無法形成VPN負載平衡(VPN LB)集群。裝置會反複遇到連線故障，如調試輸出所示：

```
device# debug vpnlb 125
debug vpnlb enabled at level 125
device# 5718045: Created peer[198.51.100.1]
5718012: Sent HELLO request to [198.51.100.1]
5718061: Inbound socket read fail: context=0.
7718036: Process timeout for req-type[13], exid[304], peer[198.51.100.1]
6718038: Slave processed 1 timeouts
5718028: Send OOS indicator failure to [198.51.100.1]
5718056: Deleted Master peer, IP 198.51.100.1
5718044: Deleted peer[198.51.100.1]
7718017: Got timeout for unknown peer[198.51.100.1] msg type[25]
```

禁用群集加密後，VPN負載平衡群集將成功形成。但是，重新啟用加密會導致群集形成失敗，並且儘管配置已完成，但不會顯示任何IKEv1調試消息。

這個問題只影響組內成員間的協調；遠端訪問VPN客戶端會話不會被丟棄。在升級之前，受影響的集群成員不會參與VPN負載平衡。

環境

- Cisco安全防火牆ASA或FTD
- ASA或FTD軟體版本包含針對強化版本的修復程式：2026年9月
- 啟用了集群加密的VPN負載平衡配置
- 為群集通訊配置的IKEv1策略

解析

有兩個經過驗證的選項可用於解決此問題：

選項 1:完成升級（推薦）

將所有集群成員升級到相同的ASA或FTD軟體版本。所有成員運行同一版本後，群集將自動進行改革。

在升級所有群整合員之前，運行舊版本的成員與運行新版本的成員保持不同步。

步驟 1:驗證所有群整合員上的當前軟體版本：

```
device# show version
```

步驟 2:將剩餘群整合員升級到相同的ASA或FTD軟體版本。

步驟 3:完成所有升級後驗證群集的形成：

```
device# show vpn load-balancing
```

選項 2:無中斷升級方法（僅限ASA）

在升級過程中臨時刪除所有成員上的群集金鑰，然後在升級所有裝置後重新應用。

步驟 1:從所有集群成員中刪除集群金鑰：

```
device(config)# vpn load-balancing
device(config-load-balancing)# no cluster key
```

步驟 2:將所有群整合員升級到相同的ASA軟體版本。

步驟 3:升級完成後，在所有成員上重新應用群集金鑰：

```
device(config)# vpn load-balancing
device(config-load-balancing)# cluster key your-cluster-key
```

重要：僅刪除群集加密是不夠的 — 在升級過程中必須完全刪除群集金鑰。

此解決方法不適用於FTD裝置，因為加密對於FMC管理的FTD裝置是強制性的。

驗證步驟

實施任一選項後，驗證群集操作是否正確。

步驟 1:驗證所有群整合員上的當前軟體版本：

```
device# show version
```

步驟 2:驗證所有升級完成後是否已形成集群：

```
device# show vpn load-balancing
```

步驟 3:驗證對等連線：

```
device# debug vpnlb 125
```

步驟 4:如果已啟用加密，請確認已建立IKEv1 SA:

```
device# show crypto ikev1 sa
```

請注意「Cisco bug ID CSCww64385」。 此問題會影響拓撲可見性和重新收斂時間，但不會影響已升級裝置上的活動VPN連線或流量轉發。

原因

此問題是由將身份驗證新增到VPN負載平衡群整合員間通訊的安全強化引起的。增強的安全協定與早期的ASA或FTD版本不相容，從而阻止在混合版本部署中形成集群。這會導致協定不相容，其中：

- 升級的節點強制實施經過身份驗證的v5協定
- 升級前節點使用未經驗證的v4協定
- 已升級的成員需要老成員無法與之通訊的強化協定
- 集群形成失敗，直到所有成員都使用相同的協定版本

相關內容

- '思科錯誤ID CSCww64385'
- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。